

EDU-2190

# Investigating Threats with Advanced Analytics

## Overview

Unlock the power of Exabeam Advanced Analytics in a one-day, instructor-led course designed to equip cybersecurity professionals with the skills to investigate and respond effectively to a range of security threats. This hands-on training program delves into the intricacies of Exabeam's analytics platform, focusing on its capabilities in identifying and mitigating compromised credentials, lateral movement, insider threats, and other types of cyberattacks. Participants will engage in hands-on labs throughout the course, applying knowledge gained to real-world scenarios. Labs include simulated investigations and response exercises, allowing participants to hone their skills in a controlled environment.

## Objectives

Students will practice investigating specific use cases that they can then translate into their own security objectives and needs. They will learn how to align Advanced Analytics with their organization's security priorities, focusing first on outcomes. Students will be challenged to demonstrate their comprehension throughout the course with the help of a course assessment, in-class activities, and lab exercises.

### At the end of this course, students will be able to:

- Describe how to achieve security outcomes using Advanced Analytics
- Begin translating common investigation workflows into Advanced Analytics, starting with these Exabeam use case categories:
  - Compromised Insiders
  - Malicious Insiders
  - External Threats (malware, phishing, etc.)
- Recall how Case Manager and Incident Responder work in Advanced Analytics to help streamline and automate incident response for greater security
- Describe how data moves through Advanced Analytics and enables detections and investigations
- Access additional educational resources in the Exabeam Training Center and Exabeam Community for more learning and professional development

## Details

Duration	Role	Modality	Level
One day	Analyst	Instructor-led	Advanced

### Prerequisites

- **Required** Complete the following courses:
  - Common Information Model (CIM) (eLearning)
  - Using Advanced Analytics (instructor-led)
- **Recommended** Experience in security tools, threat hunting, malware analysis, networking, or system administration is especially helpful.

**Intended Audience** This course is tailored for cybersecurity professionals, incident responders, security engineers, and threat hunters who wish to enhance their expertise in utilizing Exabeam Advanced Analytics for investigating and responding to security incidents.

### Training Credits 1

## Outline

### **Module 1: Get Started Operationalizing Advanced Analytics -**

Overview of the course and its key takeaways

### **Module 2: Explore the Data Flow in Advanced Analytics -**

Answers basic questions about how Advanced Analytics assigns risk scores and builds the Smart Timeline; includes an introduction to Advanced Analytics interface and main features

### **Module 3: Investigating External Threats -**

Gaining proficiency with Notable Users, Notable Assets, watchlists, and Threat Hunter

### **Module 4: Investigating Compromised Insiders and Malicious Insiders**

- An important conversation about the analyst's workflow. Includes how to use the incident lists in Case Manager; includes hands-on practice investigating an event in Advanced Analytics from end to end.